RSAC 2025 Conference

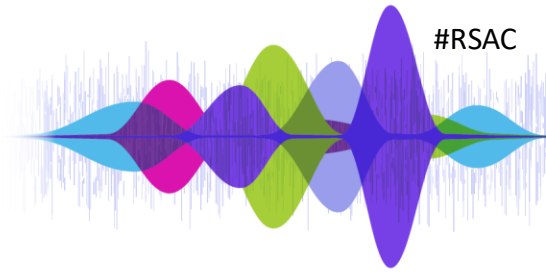
Many Voices.
One Community.

SESSION ID: IMT-M03

10 Common Flaws in Incident Response Plans

Alex Waintraub

Senior Director of CyberSecurity
VMG Health
https://www.linkedin.com/in/alexwaintraub/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Action Plan

- Who is Alex Waintraub
- Introduction
  - Laying the foundation of Incident Response
- What is an Incident Response Plan
  - Understanding the definition and necessity of an Incident Response Plan.
- Top 10 IRP Flaws & Best Practices
- Conclusion

Alex Waintraub

- Senior Director of CyberSecurity @ *VMG Health*
- Director of SOC @ *Simulint*
  - Advisory @ *Rotate*
  - Advisory @ *Tributech*
  - Contributor @ *Safehouse Initiative*
  - Navigator @ *Empath MSP*
  - Previously Worked @ *CYGNVS, Arete, BNY Mellon, Booz Allen Hamilton*

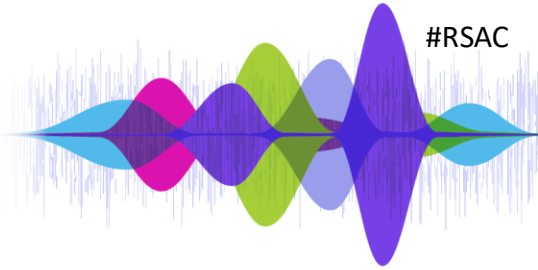
Introduction

- **Cyber Attacks are Inevitable**
  - Organizations must prepare for attacks, transitioning from 'if' to 'when'.
- **Low Preparedness Rates**
  - In 2023, F-Secure reported **only 45**% of businesses HAD an Incident Response Plan!
- **Historical Comparison**
  - IBM's 2019 report showed only **33**% with plans, indicating slow growth in readiness.
- **Common Flaws Persist**
  - Many organizations struggle with flaws in their plans, impacting recovery efforts.
- **Focus of Presentation**
  - This presentation will explore the top ten flaws in incident response plans.

"There are only two type of companies in the world: those that have been breached and know it, and those that have been breached and dont know it."

– Ted Schlein

What is an Incident Response Plan?



CISA Definition

- Defines Roles and Responsibilities
- Guides Key Activities
- Includes Key Personnel
- Establishes Communication Strategies
- Proactive and Strategic Framework

Flaw #1: Failing to Plan

If you fail to plan, you are planning to fail

- Identify and prioritize your organization's biggest risks to focus your incident response planning efforts.
- Preparation is the key to your incident response plan. No matter what you think, you can never over-prepare for the unexpected.

Flaw #2: Unclear Roles and Responsibilities

Flaw #3: Siloed Communication Strategies

Flaw #4: Inadequate Communication Strategy

Flaw #5: Neglecting Legal and Regulatory Compliance

Flaw #6: Inadequate External Third-Party Engagement

Flaw #7: Static Incident Response Plans

Flaw #8: Failure to Consider Worst-Case Scenarios

Flaw #9: Lack of IRP Testing

Flaw #10: The Ineffective Plan Execution

“Apply” Slide

Identify + Mitigate = Resilient IR Plan

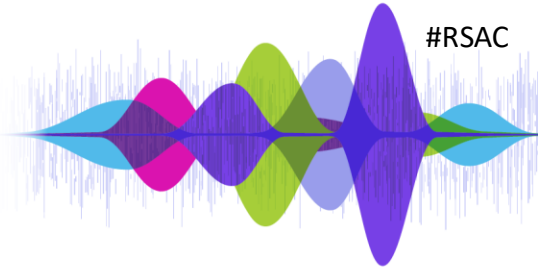
Identify the flaws: Understand the common IR flaws

Mitigate the Risks: Proactive strategies to fix weaknesses

Strengthen your Response: Testing and Execution Improvements!

Every Organization Must Test and Refine Their IR Plan!

Prepare + Test = *Effective Incident Response*



- Next week you should:
  - Review your current IR Plan for gaps.
  - Identify Key stakeholders in your IR process.
- In the first three months following this presentation you should:
  - Conduct a tabletop exercise to test your IR Plan
  - Define Roles & Responsibilities in case of an incident
  - Establish an IR Communication plan
- Within six months you should:
  - Implement regular IR plan testing and reviews
  - Engage external experts for IR Retainer services

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!

For More Information:

Contact me @ Alex.Waintraub@vmghealth.com